Administration Guide

SafeWord® Agent for Terminal Services

Version 2.1
Copyright
© 2004 Secure Computing Corporation. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Secure Computing Corporation.

Trademarks
Secure Computing, SafeWord, Sidewinder, SmartFilter, SofToken, Type Enforcement, and Strikeback are trademarks of Secure Computing Corporation, registered in the U.S. Patent and Trademark Office and in other countries. PremierAccess, G2 Firewall, G2 Enterprise Manager, Gauntlet, SecureOS, and MobilePass are trademarks of Secure Computing Corporation. All other trademarks, tradenames, service marks, service names, product names, and images mentioned and/or used herein belong to their respective owners.

Software License Agreement
The following is a copy of the Software License Agreement as shown in the software:

CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE LOADING THE SOFTWARE. BY CLICKING "I ACCEPT" BELOW, OR BY INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE, YOU ARE SIGNING THIS AGREEMENT, THEREBY BECOMING BOUND BY ITS TERMS. IF YOU DO NOT AGREE WITH THIS AGREEMENT, THEN CLICK "I DO NOT ACCEPT" BELOW AND RETURN ALL COPIES OF THE SOFTWARE AND DOCUMENTATION TO SECURE COMPUTING CORPORATION ("SECURE COMPUTING") OR THE RESELLER FROM WHOM YOU OBTAINED THE SOFTWARE.

If this Software is being installed by a third party (for example, a value-added reseller, consultant, employee, or agent), such third party represents that it has the authority to bind the person or entity for whom the Software is being installed, and that its acceptance of this Agreement in the manner set forth above does bind such person or entity.

1. Grant of License. Secure Computing grants to you, and you accept, a non-exclusive, and non-transferable license (without right to sub-license) to use the Software Products as defined herein.

2. Software Products. "Software Product(s)" means (i) the machine-readable object-code versions of software contained in the media (the "Software"), (ii) the published user manuals and documentation that are made available for the Software (the "Documentation"), and (iii) any updates or revisions of the Software or Documentation that you may receive (the "Update"). Under no circumstances will you receive any source code of the Software. Software Products provided for use as "backup" in the event of failure of a primary unit may be used only to replace the primary unit after a failure in fact occurs. They may not be used to provide any capability in addition to the functioning primary system that they backup.

3. Limitation of Use. You may not: 1) copy, except to make one copy of the Software solely for back-up or archival purposes; 2) transfer, distribute, rent, lease or sublicense all or any portion of the Software Product to any third party; 3) translate, modify, adapt, decompile, disassemble, or reverse engineer any Software Product in whole or in part; or 4) modify or prepare derivative works of the Software Products.

4. Limited Warranty and Remedies. Secure Computing warrants that the medium/media on which its Software is recorded is/are free from defects in material and workmanship under normal use and service for a period of ninety (90) days from the date of shipment to you.
Secure Computing does not warrant that the functions contained in the Software will meet your requirements or that operation of the program will be uninterrupted or error-free. The Software is furnished "AS IS" and without warranty as to the performance or results you may obtain by using the Software. The entire risk as to the results and performance of the Software is assumed by you. If you do not receive media which is free from defects in materials and workmanship during the 90-day warranty period, you will receive a refund for the amount paid for the Software Product returned.

5. Limitation Of Warranty And Remedies. THE WARRANTIES STATED HEREIN ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES AND COUNTRIES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS WHICH VARY BY STATE OR COUNTRY.
SECURE COMPUTING'S AND ITS LICENSORS ENTIRE LIABILITY UNDER, FOR BREACH OF, OR ARISING OUT OF
THIS AGREEMENT, IS LIMITED TO A REFUND OF THE PURCHASE PRICE OF THE PRODUCT OR SERVICE THAT
GAVE RISE TO THE CLAIM. IN NO EVENT SHALL SECURE COMPUTING OR ITS LICENSORS BE LIABLE FOR YOUR
COST OF PROCURING SUBSTITUTE GOODS. IN NO EVENT WILL SECURE COMPUTING OR ITS LICENSORS BE
LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY, OR OTHER DAMAGES
WHETHER OR NOT SECURE COMPUTING HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

6. Term and Termination. This license is effective until terminated. You may terminate it at any time by destroying
the Software Product, including all computer programs and documentation, and erasing any copies residing on
computer equipment. This Agreement also will automatically terminate if you do not comply with any terms or
conditions of this Agreement. Upon such termination you agree to destroy the Software Product and erase all copies
residing on computer equipment.

7. Ownership. This Software is licensed (not sold) to you. All intellectual property rights including trademarks, service
marks, copyrights, trade secrets, and other proprietary rights in or related to the Software Products are and will
remain the property of Secure Computing or its licensors, whether or not specifically recognized or protected under
local law. You will not remove any product identification, copyright notices, or other legends set forth on the Software
Product.

8. Export Restrictions. You agree to comply with all applicable United States export control laws and regulations,
including without limitation, the laws and regulations administered by the United States Department of Commerce and
the United States Department of State.

9. U.S. Government Rights. Software Products furnished to the U.S. Government are provided on these commercial
terms and conditions as set forth in DFARS 227.7202-1(a).

10. Entire Agreement. This Agreement is our offer to license the Software Product to you exclusively on the terms set
forth in this Agreement, and is subject to the condition that you accept these terms in their entirety. If you have
submitted (or hereafter submit) different, additional, or other alternative terms to Secure Computing or any reseller or
authorized dealer, whether through a purchase order or otherwise, we object to and reject those terms. Without
limiting the generality of the foregoing, to the extent that you have submitted a purchase order for the Software
Product, any shipment to you of the Software Product is not an acceptance of your purchase order, but rather is a
counteroffer subject to your acceptance of this Agreement without any objections or modifications by you. To the
extent that we are deemed to have formed a contract with you related to the Software Product prior to your acceptance
of this Agreement, this Agreement shall govern and shall be deemed to be a modification of any prior terms in their
entirety.

11. General. Any waiver of or modification to the terms of this Agreement will not be effective unless executed in
writing and signed by Secure Computing. If any provision of this Agreement is held to be unenforceable, in whole or
in part, such holding shall not affect the validity of the other provisions of this Agreement. You may not assign this
License or any associated transactions without the written consent of Secure Computing. This License shall be
governed by and construed in accordance with the laws of California, without regard to its conflicts of laws provisions.
Technical Support information
Secure Computing works closely with our Channel Partners to offer worldwide Technical Support services. If you purchased this product through a Secure Computing Channel Partner, please contact your reseller directly for support needs.

To contact Secure Computing Technical Support directly, telephone +1.800.700.8328 or +1.651.628.1500. If you prefer, send an e-mail to support@securecomputing.com. To inquire about obtaining a support contract, refer to our “Contact Secure” Web page for the latest information at www.securecomputing.com.

Customer Advocate information
To suggest enhancements in a product or service, or to request assistance in resolving a problem, please contact a Customer Advocate at +1.877.851.9080. If you prefer, send an e-mail to customer_advocate@securecomputing.com.

If you have comments or suggestions you would like to make regarding this document or any other Secure Computing document, please send an e-mail to techpubs@securecomputing.com.

Printing history

<table>
<thead>
<tr>
<th>Date</th>
<th>Part number</th>
<th>Software Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 2002</td>
<td>86-0936754-A</td>
<td>SafeWord Agent for Terminal Services, Version 1.1</td>
</tr>
<tr>
<td>July 2003</td>
<td>86-0936754-B</td>
<td>SafeWord Agent for Terminal Services, Version 2.0</td>
</tr>
<tr>
<td>September 2004</td>
<td>86-0936754-C</td>
<td>SafeWord Agent for Terminal Services, Version 2.1</td>
</tr>
</tbody>
</table>
Using SafeWord® Agent for Terminal Services

About this document

This document describes how to set up and use the SafeWord Agent for Terminal Services. It is intended for use by the person responsible for administering their organization’s network and its users.

This document contains the following topics:

- “Overview” on page 2
- “Operating system requirements” on page 3
- “Special deployment considerations” on page 3
- “Installing SafeWord Agent for Terminal Services” on page 4
- “Using the Configuration Utility” on page 8
- “User login after installing SafeWord Agent for Terminal Services” on page 12
- “Locking and unlocking your Server Console” on page 14
- “Uninstalling SafeWord Agent for Terminal Services” on page 14
- “Troubleshooting” on page 14
Overview

The SafeWord Agent for Terminal Services is a security enhancement add-on to a “Terminal Services” environment, providing strong authentication for both remote and console user logon attempts.

**Important:** In this document, “Terminal Services” means either the **Terminal Services for Windows 2000/2003/XP** environment or the **Citrix Metaframe for Windows 2000** environment. (Specific operating system requirements are listed on page 3.)

In Figure 1, a user attempts entry into the terminal services environment. Their user name is passed to the Windows 2000 domain controller for normal Windows authentication against the appropriate database.

![Figure 1. Basic flow for SafeWord Agent for Terminal Services authentication request](image-url)
To pass authentication, the user must pass both Windows authentication and (possibly) strong authentication. Once the user provides the correct Windows credentials, they are checked against the Authentication Policy (as defined by the administrator in the configuration utility) to see if further authentication is required. If so, their machine’s name (or IP address) are compared against the Host Exclusion List for possible exclusion.

If the Authentication Policy requires further authentication and they are not excluded by the Host Exclusion List, they are required to pass strong authentication. Only after passing both Windows authentication and strong authentication (if required) will they be granted access to the Terminal Service (or Citrix) machine. SafeWord Agent for Terminal Services supports fixed passwords, tokens, and software authenticators.

**Operating system requirements**

SafeWord Agent for Terminal Services works with the following operating systems:

- Windows 2000/2003/XP Server with MetaFrame installed
- Windows 2000/2003/XP Server with Terminal Services installed

**Note:** If using SafeWord Agent for Terminal Services on a network with the SafeWord Agent for Windows Domains, the Terminal Server must be added to the SafeWord Agent for Windows Domains’ configuration file’s property sheet (found in the “Host Exclusions” list). This is an architecture/design issue with Windows Domain Security, and Secure Computing products.

**Special deployment considerations**

**Note:** If you specify that users require authentication based on a per-group basis in the Authentication Policy and the group look-up method is set to query Domain Controller, then the following paragraph applies.

If you are installing SafeWord Agent for Terminal Services to protect applications on a Windows 2000 domain, you must make the machine on which it is installed a member server on the domain. Also, if the Citrix server is installed in a member server on a domain (resource domain) and the user records are in a different domain, you must have a two way trust relationship for the agent to work properly.
Installing SafeWord Agent for Terminal Services

This section describes how to install and configure the SafeWord Agent for Terminal Services. The agent is included on the Deployment CD that ships with PremierAccess. It can be installed from the CD or it can be downloaded from the Secure Computing Web site.

**Important:** You must have a PremierAccess™ server in your network prior to installing the SafeWord Agent for Terminal Services. You must have Administrator privileges to install the Agent for Terminal Services. Administrator privileges are required to write entries into the registry. Attempting to install the software without Administrator privileges will result in automatic termination of the install program.

Installing the agent from the Deployment CD

If you are installing from the Deployment CD, insert the CD into your computer's disc drive and follow the prompts to install the agent. When prompted, supply the host name (or IP address) and port number for the SafeWord PremierAccess server.

**Note:** Specify port 5031 for EASSP protocol 201 or 5030 for EASSP protocol 101.

When the installation is complete, reboot the system on which you have just installed Terminal Services. You must reboot your system before SafeWord Agent for Terminal Services will load or run.

**Important:** Physical security of the Terminal Services/Citrix server console is very important. Failure to restrict access to the server console can result in a compromise of the network protection that SafeWord Agent for Terminal Services is designed to offer. Refer to “Setting access restrictions” on page 6.

Downloading and installing the agent from the Web

To download the agent from Secure Computing’s Web site:

1. Go to [www.securecomputing.com](http://www.securecomputing.com).
   
   
   b. Click on SafeWord® PremierAccess™ Agents.
   
   c. Scroll down to the SafeWord® PremierAccess™ Agents section.
   
   d. Scroll down to the Windows Agents section, and click on the Download Agent for Terminal Services link. A dialog box appears informing you that you are downloading the Terminal Services Agent from [www.securecomputing.com](http://www.securecomputing.com), and asks if you want to open the file, or save it to your computer.
Installing SafeWord Agent for Terminal Services

e. Click *Save*. When the Save As window appears, choose the location to which the Terminal Services Agent executable will be saved.

f. Click *Save*. The compressed file, named `swagent4tsx.exe` will be saved to the chosen directory.

g. Locate the downloaded file, and double-click to extract the source components. Save the extracted files to the desired directory.

2. Locate and double-click `setup.exe` file. The autorun sequence begins. Follow the onscreen prompts.

3. When prompted, supply the host name (or IP address) and port number for the SafeWord PremierAccess server.

   **Note:** Specify port 5031 for EASSP protocol 201 or 5030 for EASSP protocol 101.

4. Reboot the system on which you have just installed Terminal Services. You must reboot your system before SafeWord Agent for Terminal Services will load or run.

   **Important:** Physical security of the Terminal Services/Citrix server console is very important. Failure to restrict access to the server console can result in a compromise of the network protection that SafeWord Agent for Terminal Services is designed to offer.
Setting access restrictions

Access restrictions within an environment protected by Terminal Services can be tightly controlled by setting Authentication Policy and Host Exclusion parameters in the Configuration Utility (see “Using the Configuration Utility” on page 8). The Authentication Policy and Host Exclusion work together to form the basic access rights for users.

Authentication Policy applies to users. It allows you to specify whether a user (all or remote) or group of users (all in a group or all not in a group) will be required to provide PremierAccess credentials. If a user matches an Authentication Policy parameter, then the Host Exclusion parameters are used for further restrictions.

Host Exclusion applies to client machines. It allows you to specify machines (by IP address, machine name, or range of IP addresses) from which users can log into a protected system using normal Windows authentication, but without supplying PremierAccess credentials. Figure 2 on page 6 and Table 1 on page 7 work together to illustrate the concepts described above.

In Figure 2, User 1 is logged onto remote Machine 1. In Table 1 (first row), the Authentication Policy (AP) is set to “All Remote,” and the Host Exclusion (HE) is set to Disable. Since the AP requires all remote users to pass strong authentication, the HE list is consulted for further restrictions, and is set to Disable (which counts as a yes). Since the AP and HE work together as logical AND operands, and both require strong authentication, the final requirement for strong authentication becomes a Yes (Y AND Y = Y). If both AP and HE equal Yes, then the final will always be Yes.
Table 1. Authentication setting table (use with Figure 2)

<table>
<thead>
<tr>
<th>If User...</th>
<th>...is logged on Machine (M)...</th>
<th>...with Authentication Policy (AP) set to...</th>
<th>...and the Host Exclusion (HE) set to...</th>
<th>...then if Strong Authentication is required by...</th>
<th>The Final req. is...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Disable</td>
<td>Require if M2</td>
<td>AP?</td>
<td>HE?</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>All remote</td>
<td>Exclude if M1</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td></td>
<td>Require if M2</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>TS</td>
<td></td>
<td>Disable</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>All users</td>
<td>Exclude if M1</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td></td>
<td>Require if M2</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>TS</td>
<td></td>
<td>Disable</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>1</td>
<td>All users in group: SAFEWORD_USERS</td>
<td>Require if M2</td>
<td>Exclude if M1</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Disable</td>
<td>Exclude if M1</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>TS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>Exclude if M1</td>
<td></td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Exclude if M1</td>
<td></td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>TS</td>
<td>All users NOT in group: SAFEWORD_USERS</td>
<td>Exclude if M1</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
Using the Configuration Utility

A Terminal Services installation also includes a configuration utility that is launched under the Windows Start menu. With it you can set user strong authentication requirements, specify machine names and/or IP addresses if strong authentication is required, the name or IP address and port number of the authentication server which provides authentication verification, and debug settings for filtering log files.

To launch the configuration utility, from the Start menu, select Start -> Programs -> Secure Computing -> SafeWord Agent for Terminal Services -> Configure TS Agent. The configuration utility appears, showing the Authentication Policy tab by default.

In this pane you will set the policy which determines whether a user (or group of users) is required to provide PremierAccess credentials. If a user matches the settings in this pane, the Host Exclusions settings are referred to for further restrictions.

1. Set one of the following user configurations:

   - **Per User Basis: ALL REMOTE USERS**: requires strong authentication for users logging on remotely.
   - **Per User Basis: ALL USERS**: requires strong authentication for all users.
   - **Lockout** “Back door” credential: If the policy requires all users to pass strong authentication but the authentication server is down...
or unavailable, this reserved name and password can be used to bypass the authentication server and permit access. The Name field must be populated with a valid Windows “user” account name (set up for this specific purpose) and be able to pass normal Windows authentication. Since this feature uses a simple fixed password, care must be taken to assign a password of sufficient complexity to reduce the chance of being guessed.

- **Per Group Basis: ALL USERS IN GROUP:** requires strong authentication for all users assigned to the group listed in the Name of the group field.
- **Per Group Basis: ALL USERS NOT IN GROUP:** applies to all (otherwise) grouped users who are not part of the group listed in the Name of the group field.
- **Method for group lookup: Use Logon session information:** (recommended) obtains group information from the Windows authentication.
- **Method for group lookup: Query domain controller:** this method is less desirable as some cases exist in which the agent may have difficulty retrieving group information from a domain controller, and authentication would fail.
- **None:** disables the agent, but leaves all settings intact.

2. When the desired choices have been made, click the **Host Exclusion List** tab.

The Host Exclusion List works with the Authentication Policy pane to create the following logical AND condition:

- If the authentication policy requires strong authentication for a user,
- AND the Host Exclusion List does not exclude the user’s machine,
- THEN the user must pass strong authentication.
If a user is not required by the Authentication Policy to pass strong authentication, they can still log into a protected system from specific client machines (after passing normal Windows authentication) if the machine from which the logon attempt is being made is listed in the Host Exclusion list.

The client machines listed in this pane (by machine name, IP address, or range of IP addresses) can either be required or excluded from the need to provide strong authentication.

3. Enter machine name(s) or IP address(es) to be considered under this policy.
4. Click the appropriate radio button to determine if the listed machine(s) will be **Excluded** from authentication, or **Required** to authenticate.
5. (Optional) Click the **Disable** radio button to turn this exclusion feature off.
6. When finished, click the **AAA Server Information** tab.

In this pane you can enter the name (or IP address) and port number of the authentication server to which the Terminal Services agent will forward all requests for verification. You will also specify the EASSP protocol to be used.
7. Enter the name (or IP address) and port number for the authentication server.

The port number you enter will be determined by the protocol you will be using. Use port number 5031 for protocol 201, or port number 5030 for protocol 101.

8. Enter the appropriate protocol to be used.

9. When finished, click the Debug Settings tab.

![Figure 6. Terminal Services Configuration Utility, Debug Settings tab](image)

This pane allows you to determine what sorts of logs are generated and sent to the log file, and the log file size limit before it is automatically archived and a new log file is generated.

10. Set the Event Log and File type(s):

   - **None**: no logs are generated.
   - **Error**: only events considered errors are sent to the log file.
   - **Info**: routine informational messages are sent to the log file.
   - **Debug**: all event types are sent to the log file. This option is considered highly verbose, and can quickly result in large log file sizes.

11. Set the File Name for the log file.

    Either enter the entire pathname, or use the Browse button to locate a specific directory into which the log file will be stored.

12. Set the Max File Size for the log file.
User login after installing SafeWord Agent for Terminal Services

Once the log file reaches the size limit you set, it will automatically be archived, and a new log file will be created.

13. Click OK when you have set, and are satisfied with all configurations in this utility.

User login after installing SafeWord Agent for Terminal Services

Once SafeWord Agent for Terminal Services is installed, users attempting to login (either from the local or remote machine) will see a login window requesting their user login information (refer to Figure 7).

Note: The following windows are specific to the Windows 2000 environments.

![Figure 7. Initial login window](image)

The login window contains input fields for user credentials (user name, password, and domain). Upon entry, these credentials are passed to the Domain Controller for an initial pass through the Windows Active Directory database. If the username passes Active Directory database authentication, and does not require additional strong authentication, entries made in the password field are ignored and they’re passed on through to the network.

Note: An entry into the SafeWord Password field is only required in cases where they need an additional level of authentication.
If the user requires strong authentication and no password had been supplied (bottom field in the above window), then the following window appears.

**Figure 8. SafeWord user input window**

![SafeWord User Input](image)

Figure 8 shows the prompt for a fixed password. If some other type of authentication is required for this user (e.g., hardware authenticator, or combination of hardware/software authenticators), the dynamic prompt field will display the appropriate prompt.

If the authentication process fails for any reason, the user is notified that an authentication error occurred.

**Figure 9. SafeWord Authentication failure window**

![SafeWord Information](image)

In this case, the user will be returned to the initial login window and prompted for all required information.

In some cases, an advisory message window may appear in which additional information (such as the impending password expiration, or an access attempt using their password) may need to be relayed to a user.
Locking and unlocking your Server Console

As with a normal Windows 2000 workstation, your users can lock and unlock their workstation by using the Ctrl->Alt->Delete keystroke combination. Trying to unlock a locked server with SafeWord Agent for Terminal Services installed will display a window that prompts for user ID and password.

Uninstalling SafeWord Agent for Terminal Services

To uninstall SafeWord Agent for Terminal Services, do the following:

1. In the Windows Start menu, select Start -> Settings -> Control Panel.
2. Click Add/Remove Programs.
4. Reboot the system.

Troubleshooting

This section gives you an overview of the SafeWord Agent for Terminal Services authentication flow process, as well as information to help you troubleshoot problems that you may encounter.

Figure 11 provides a visual representation of the SafeWord Agent for Terminal Services authentication process. You may find this diagram particularly helpful if you need to run troubleshooting procedures.
Troubleshooting

Using SafeWord® Agent for Terminal Services

Figure 11. SafeWord Agent for Terminal Services flowchart

Errors such as "Cannot find DC" or "cannot get group info"

Bad new password?

Change password?

Authenticator pass?

Check authenticator combos

Get config file, open server

Windows Authentication

Pass?

Yes

Policy requires PA Authentication?

Yes

Fail

Bad ID

Failed Authentication

Locked

Record Locked

No

Pass

More authenticators?

Yes

No

Policy requires PA Authentication?

Yes

No

Pass

Fail

Retry

No

Policy requires PA Authentication?

Yes

No

Pass

Fail

Retry

More authenticators?

Yes

No

Change password?

Yes

No

Pass

Fail

Retry

More authenticators?

Yes

No

Policy requires PA Authentication?

Yes

No

Pass

Fail

Retry

More authenticators?

Yes

No

Policy requires PA Authentication?

Yes

No

Pass

Fail

Retry

More authenticators?
## Troubleshooting

### Problems and possible causes

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>User fails login</td>
<td><strong>Note:</strong> If your Authentication Policy specifies that users require authentication based on a per-group basis and the group lookup method is set to query Domain Controller, then the following applies.</td>
</tr>
<tr>
<td></td>
<td>• User aborted logon prior to completing authentication</td>
</tr>
<tr>
<td></td>
<td>• Failed normal Windows 2000 authentication (at local machine); wrong password</td>
</tr>
<tr>
<td></td>
<td>• Local machine is unreachable for SAFEWORD_USERS group queries</td>
</tr>
<tr>
<td></td>
<td>• Check the following:</td>
</tr>
<tr>
<td></td>
<td>• the domain controller lacks two-way trusts</td>
</tr>
<tr>
<td></td>
<td>• the Terminal Services Agent machine is a domain controller</td>
</tr>
<tr>
<td></td>
<td>• the domain is a layered domain topology</td>
</tr>
<tr>
<td>User fails PremierAccess authentication</td>
<td>• Cannot find libswecapi.dll or SccTermSrv.cfg files in &lt;WinDir&gt;\SYSTEM32 directory</td>
</tr>
<tr>
<td></td>
<td>• Database being modified (for example, attack lock, time/day/week, etc.)</td>
</tr>
<tr>
<td></td>
<td>• Wrong/invalid password</td>
</tr>
<tr>
<td></td>
<td>• Changing fixed password failed; wrong old password, abort, bad new password</td>
</tr>
<tr>
<td></td>
<td>• Bad swec.md5 (for EASSP201) or swec.dat (for EASSP101) file created in &lt;Windir&gt;\system32</td>
</tr>
<tr>
<td></td>
<td>• Delete swec.md5 (or swec.dat) file</td>
</tr>
<tr>
<td></td>
<td>• Login using dynamic password</td>
</tr>
<tr>
<td>Authentication server unreachable</td>
<td>• Verify the following SccTermSrv.cfg configurations:</td>
</tr>
<tr>
<td></td>
<td>• Verify that the authentication server is running.</td>
</tr>
<tr>
<td></td>
<td>• Verify host name or IP address of the authentication server. If host name is used, try IP address in case the DNS entry for the host name is missing or incorrect.</td>
</tr>
<tr>
<td></td>
<td>• Verify authentication server port number in line 02.</td>
</tr>
<tr>
<td></td>
<td>• Verify authentication server port number matches EASSP Protocol # in line 55.</td>
</tr>
</tbody>
</table>

More...
The `SccTermSrv.cfg` file

This file determines several operating parameters for SafeWord Agent for Terminal Services. For example, during installation you enter the host name (or IP address) and port number of the PremierAccess server, which is then written to the `SccTermSrv.cfg` file, located at `<WinDIR>\SYSTEM32\SccTermSrv.cfg`. If either of those entries are wrong, the PremierAccess server will be unreachable.

The `SccTermSrv.cfg` file can be edited using any text editor. All values are case sensitive. Lines beginning with a pound sign (#) are treated as comments (# must be the first character of the line).

Each line in the file has two parts:

<table>
<thead>
<tr>
<th>Parameter descriptor</th>
<th>Parameter value</th>
</tr>
</thead>
<tbody>
<tr>
<td>02 SafeWord Auth Server : 192.168.1.1 0 0 5031</td>
<td></td>
</tr>
</tbody>
</table>

**Parameter descriptor**

Text to the left of the colon is a parameter descriptor. It must include a two character ID (for example, 02 as above) at the beginning of the line, followed by a space. The remaining text portion of the descriptor is only used to make the entry “human readable.”

**Parameter value**

Text to the right of the colon is the actual parameter value.

An incorrect PremierAccess server Hostname (or IP address), or port number can be corrected by editing the incorrect value in `SccTermSrv.cfg` file.
Syntax for *SccTermSrv.cfg* file entries specific to the PremierAccess server is:

02 SafeWord Auth Server: host wt=0 connections=0 [port]

An entry would look like this:

02 SafeWord Auth Server : 192.168.1.1 0 0 5031

55 EASSP Protocol: 201

*Note:* Specify port 5031 for EASSP protocol 201 or 5030 for EASSP protocol 101.

---

**LogFile/EventLog Messages**

The *SccTermSrv.cfg* file can record error, informational, debug, and status messages to the `<WinDIR>\SYSTEM32\SccTermSrv.log` file and/or `eventLog`. Normally, this value is set to **error**.

Valid entries are:

- **NONE:** no logging is sent
- **ERROR:** error messages are sent
- **INFO:** routine informational messages are sent
- **DEBUG:** debugging messages are sent

More than one type of message can be specified as in:

15 Send Status Messages to User: ERROR INFO